DOCUMENT RESUME

ED 307 853 IR 013 819

TITLE	Information Technology Issues. Transition Series.
INSTITUTION	Comptroller General of the U.S., Washington, D.C.
REPORT NO	GAO/OCG-89-6TR
PUB DATE	Nov 88
NOTE	28p.
AVAILABLE FROM	U.S. General Accounting Office, P.O. Box 6015, Gaithersburg, MD 20877 (1-5 copies free).
PUB TYPE	Viewpoints (120) -- Reports - Evaluative/Feasibility (142)
EDRS PRICE	MF01/PC02 Plus Postage.
DESCRIPTORS	Access to Information; *Federal Government; *Information Management; *Information Technology; Long Range Planning; Policy Formation; *Public Policy; *Systems Development; *Technical Occupations
IDENTIFIERS	Federal Agencies; *Strategic Planning

ABSTRACT

Addressed to the new administration and the Congress, this summary report on Federal Government information management and technology issues begins by describing the environment in which information technology has been managed. Arguing that effective government depends directly on effective automation to support programs and initiatives, the report then identifies four areas that need improvement: (1) strategic planning that ties agencies' technology to their missions; (2) systems development projects that provide technical capability; (3) automated information system security that protects sensitive information; and (4) technical personnel who oversee complex automated systems. A list of related publications from the General Accounting Office is included. (EW)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

United States General Accounting Office

GAO

Transition Series

ED307853

November 1988

Information Technology Issues

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☒ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

IR013519

GAO/OCG-89-6TR

GAO

United States
General Accounting Office
Washington, D.C. 20548

Comptroller General
of the United States

B-158195

November 1988

The President of the Senate
The Speaker of the House of Representatives
The Director-designate of the Office of Management and Budget

This summary report is one of a series that addresses major policy, management, and program issues facing the new administration. The issues discussed here represent the results of GAO work in the area of information management and technology.

Effective government depends directly on effective automation to support programs and initiatives. Virtually all facets of government rely on technology, but management of this technology has been uneven. Critical areas have not been given focused attention, and major computer and telecommunications systems have met with mixed success.

The possibility for significant improvement is at hand. This report describes the environment in which information technology has been managed and identifies four areas that need attention: (1) strategic planning that ties agencies' technology to their missions, (2) systems development projects that provide technical capability, (3) security that protects sensitive information, and (4) personnel who oversee complex automated systems. These areas, all of which are undergoing rapid changes, provide vital support to government operations. The new administration and the Congress have an opportunity to make lasting improvements to government services by improving management of the technology that supports these services.

Charles A. Bowsher

Charles A. Bowsher

Contents

Letter	1
The Information Technology Environment in the Federal Government	4
Strategic Planning	9
Systems Development Projects	12
Automated Information System Security	15
Technical Personnel	18
Related GAO Products	22
Transition Series	25

The Information Technology Environment in the Federal Government

The environment in which the federal government manages its information technology is one of tensions between time, technology, cost, and talent. It is characterized by long-term projects, short-term tenures of senior and mid-level managers who often refocus program priorities, and rapid changes in technology. In addition, federal systems are often unique and extremely complex, and are acquired in an environment that is unlike private industry. Finally, the government's information technology costs are high and rapidly increasing: it is projected that about $17 billion will be spent on information technology in fiscal year 1989, as compared to $9 billion spent in 1982.

Today, information technology is essential to carrying out our nation's most vital functions. Our ability to avert war and to defend ourselves depends significantly on the strength of our computer and communications systems. Our ability to deliver social security checks to our elderly, to deliver benefits to our disabled veterans, to direct aid to needy families, all depends on the smooth operation of computer and telecommunications systems. Our nation cannot land planes safely or launch a single space vehicle without the accurate and reliable functioning of immensely complex computer technology. Our ability to raise

the revenue that pays for these services is tied to automated systems that process tax information.

The role of the federal government in managing this technology is equally important: strong, informed leadership is essential to well-functioning systems. This leadership must understand the environment in which technology operates, and the particular demands that accompany federal automation projects.

Many federal projects take a long time to implement, overlapping the administrations that manage them. A multi-billion-dollar modernization program supporting social security began in 1982. Although originally estimated to be completed in 5 years, completion is still years away. From 1982 until now, it has been developed under three commissioners or acting commissioners, some of whom have changed the system's goals and objectives. A tax system redesign, which originally began in 1968, never progressed beyond the conceptual design stage and was eventually killed in 1978. It was started anew in 1982 and will cost several billion dollars between now and 1998 when completed; this renewed effort has also undergone a number of redirections by a succession of top managers.

Dramatic changes take place in information technology between the time many of the government's systems development projects start and when they end. Small computers using advanced chip technology, powerful communications technology, and large-scale, cheap mass storage are but a few recent changes. Such advances offer possibilities to revolutionize the way the government and industry do business. By the year 2000, a little more than a decade from now, the possibilities are expected to grow even more. Rapid advances coupled with long-term projects place federal managers in a difficult and challenging position as they make choices about technology.

Many federal systems are being designed as one-of-a-kind in their size and complexity. Systems supporting aviation, veterans' programs, tax administration, social security, space programs, and defense have limited private-industry models and rival or exceed the cost, size, and complexity of the largest systems of any private firm.

The government's systems are operated in an oversight arena unparalleled in private industry. The federal government's commitment to competition has been embodied and reaffirmed in legislation such as the Brooks Act, the Paperwork Reduction Act

of 1980, and the Competition in Contracting Act. Its commitments to protect the privacy of citizens and the security of sensitive computerized information are set forth in the Privacy Act of 1974 and the Computer Security Act of 1987. The regulatory and budgetary environment is designed to provide a set of checks and balances to achieve the objectives of these acts and make sure that systems are effective and that their value is worth their cost.

The cost of the federal government's computer systems is staggering. For example, a system proposal for satellite control operations that is under study could cost $48 billion to implement between 1990 and 2015. Another project, the government's new telephone system known as FTS 2000, could cost up to $25 billion over the next 10 years.

The technological challenges facing this nation over the next few years call for strong leadership. The incoming administration, the Congress, and managers throughout the government must act together to ensure that our information technology works, and works well. Without this leadership, we cannot rely on our national defenses, no matter how dedicated our people or how sophisticated our

equipment. Without it, we cannot hope to manage our finances, provide our social services, or guarantee the safety of our transportation systems.

Our nation's leadership must address several key issues over the next few years if we are to take full advantage of our technology. We must effectively harness this technology to accomplish our government's missions. We must make sure that our systems work as planned. We must adequately protect the information in these systems. Finally, we must get and keep the talented people needed to oversee the systems. In short, to govern our nation effectively, we must manage our technology effectively.

Strategic Planning

Strategic planning for computers and telecommunications is critical to focusing an agency's use of information resources toward achieving the mission of the organization. However, in too many instances, agencies either do not complete strategic plans or develop plans that are not effective. Moreover, strategic plans are frequently not tied to agency budget requests. As a result, millions are spent on computer systems that do not meet agency needs, do not perform as desired, are not cost-effective, and are not compatible with existing and future agency systems.

Strategic plans identify an agency's mission, relate each automation program objective to this mission, state the objectives in measurable terms, and set priorities for automation efforts. Strategic plans are also important in ensuring that systems will be integrated resources that can easily communicate with each other. Integration can be achieved by establishing and enforcing standards that ensure different systems can exchange information and share complex, expensive software.

Federal agencies frequently do not use strategic planning effectively. The nation's warning and attack assessment system's unit for monitoring communications lines has design deficiencies that will preclude

its installation and use unless substantial changes are made. Besides these deficiencies, the unit is not compatible with other equipment at the operating facility.

In another case, major decisions shaping the government's planned procurement of long-distance services known as FTS 2000 have been made without adequate analysis. Because the agency did not conduct a comprehensive analysis of a range of alternatives, it was uncertain whether FTS 2000 is optimal technically, economically, or contractually.

In another instance, because plans for modernizing a worldwide military command and control system were not updated, the agency was preparing to unnecessarily spend $500 million for new computer systems. These new systems were to meet requirements that had been in most cases satisfied by previous expenditures.

Agencies do not perform effective strategic planning because top managers do not recognize its importance in directing major automation efforts. Many continue to view it as a bureaucratic exercise to comply with government regulations, rather than a necessary effort to support mission objectives.

The government needs to treat strategic planning seriously. Top-level commitment to strategic information resources planning is imperative. Specifically, agency top management needs to:

- Recognize the role and importance of strategic planning in guiding information resource activities.
- Develop, implement, and enforce strategic plans that effectively marshal information technology toward achieving the agency's mission.
- Review and update plans periodically to ensure their applicability and usefulness.
- Ensure that individual system projects are developed in accord with strategic plans.
- Ensure that strategic plans are consistent with budget requests and agency reprogramming actions.

Systems Development Projects

Some of the government's major systems development projects have had costs escalate by hundreds of millions of dollars and schedules slip by years. In many cases the new systems do not work as planned or meet user needs, and waste millions of dollars. These conditions jeopardize the government's ability to carry out some of its most fundamental missions. The following are some recent examples:

- A federal aviation system may not have been the most cost-beneficial approach because alternative system architectures were not evaluated. We estimated that a different system could reduce costs by more than $750 million.

- Evolving and expanding requirements for a defense automated financial system have caused estimated costs to grow from about $30 million to almost $500 million and schedules to slip by more than 5 years.

- Critical systems planning steps for a $1.5 billion defense logistics modernization project were not completed, making it questionable whether the system will be worth its cost, and whether it will correct existing deficiencies.

- A multi-million-dollar expansion of a system supporting veterans programs was

implemented without adequate analysis of costs and benefits. It remained questionable whether the most cost-effective system was selected.

These problems result from errors made in the early stages of a system's development. Agencies frequently do not adequately define their requirements, and therefore implement systems that do not meet users' needs. Agencies frequently do not consider less costly alternatives to the systems they select. Selected systems often are not justified, with the result that their costs greatly exceed benefits. Once program implementation is underway, problems often persist because of failure to follow approved plans, inadequate testing, inadequate supervision, and lack of management support.

Problems that arise during the development and implementation of a system can be costly and difficult to resolve. To prevent these problems, top management needs to establish good management practices to control projects through each of the system's phases: initiation, development, and operation. Specifically, agencies need to:

- Ensure that, for each systems development project, requirements are adequately

defined, alternative solutions are fully evaluated, and the costs and benefits of alternatives are assessed.

- Obtain extensive user involvement, assign and retain competent staff, promote continuing communication among managers, standardize approval processes for plans and decisions, provide for complete and accurate documentation, and establish and use appropriate management controls to make decisions on system costs and schedules.

Automated Information System Security

Estimates of the annual cost of security breaches suffered by public and private institutions range into the billions of dollars. The rapid growth of automated information systems has increased the government's exposure to these risks. Recent instances of security breaches in automated information systems have resulted in the loss of assets, compromise of program objectives, and leaks of sensitive information.

Many current automated information systems are vulnerable to a range of problems because agencies do not incorporate appropriate security controls during development, and in day-to-day operations. In our 1985 review of 25 systems at 17 civilian agencies, we testified that each of these systems is vulnerable to abuse, destruction, error, fraud, and waste because of very limited use of security controls, such as risk management and audit trails.

A 1986 Office of Technology Assessment review of 142 agency components found similar weaknesses in information security controls and management practices. In 1988 we reported that, in 9 systems development projects we reviewed, management made significant project decisions without adequate consideration of potentially important security factors.

When agencies do not incorporate appropriate controls and do not adequately consider security in system development and operations, the results can be disastrous. A clerk used a transportation computer processing system to embezzle more than $800,000. Employees prepared fraudulent documents for a tax processing system, directing refunds to themselves and others. At least 30 employees obtained illicit access to computer and data files supporting agricultural programs, and made unauthorized and premature disclosure of highly sensitive information. Some federal agencies have also been the victims of computer viruses—deliberate tampering with software—that have destroyed the integrity of their software and data.

In addition to these malicious acts, agencies remain vulnerable to acts of negligence. In one review, we reported that flaws in a social security control system caused millions of dollars in erroneous payments. We further reported that a program had provisions for field office personnel to override many of the computer system's controls, and as a result incorrect and incomplete data were entered and processed.

As recognized in the recently enacted Computer Security Act of 1987, the ever-

increasing use of automated systems has increased exposure to security breaches. In particular, the proliferation of telecommunications and personal computers has significantly increased the risk of unauthorized access to data.

The rapid pace of technology adds to these problems, making it difficult for security practices to keep up with changes. In addition, inattention to safeguards in the early stages of system design is common, with the result that systems must be retrofitted with security features. Retrofitting tends to be more costly and less effective than including safeguards during development.

High-level attention is needed to ensure an appropriate level of security for automated systems. Agency management must:

- Evaluate their current agency policies and procedures to assure that systems are developed and implemented with appropriate security controls built into the design.
- Improve mechanisms to detect security breaches, assess their significance, and report them to top-level officials.

Technical Personnel

Qualified technical personnel are needed at all levels if the government is to build and operate the automated information systems that provide essential services to the nation. At present, a governmentwide shortage of technical staff has resulted in many federal agencies not being able to meet crucial objectives. Some recent, highly publicized problems underscore these weaknesses, and the need for change.

The recent stock market crash revealed the inability of federal regulators to monitor the performance of computer systems of the various exchanges. Modernization of the social security system has been delayed by a shortage of management and support staff with the technical knowledge to implement and complete the project. A similar lack of technical expertise at the senior-management level has contributed to delays in the tax administration system.

Although this demonstrated lack of technical expertise has complex causes, there are underlying reasons for it: managers are having problems finding competent personnel, managers often lack necessary technical expertise themselves, and agencies are having problems keeping their most talented staff.

In a 1987 survey, about 40 percent of federal managers reported to us that their ability to hire needed staff had worsened over the past 5 years. Competition is particularly acute in expanding fields, such as computer science. The shortage of trained personnel is already apparent and is projected to become severe by the year 2000. Compounding these problems is the fact that the government is in the middle of a transition into services supported by high technology and needs to acquire technical expertise quickly.

The government is at a disadvantage when recruiting because government salaries fall far behind those in private industry. A Merit Systems Protection Board's recent survey found the government's entry-level salaries for computer specialists ranged from 22.7 to 31.6 percent less than those in private industry. The President's Commission on Compensation of Career Federal Executives found that private industry pays senior executives as much as 65 percent more than the government. The government is also at a disadvantage because questions are being raised about the way it defines the roles to be played by its technical personnel.

Unflattering perceptions of government employment further complicate efforts to

recruit and keep a technical work force. Our 1987 survey showed that the greatest source of dissatisfaction among senior executives is the negative rhetoric directed toward public service.

Low pay and a bad image lead to high turnover of talented personnel. Private corporations court the best government employees with offers of high salaries and attractive working conditions. The Council of Federal Data Center Directors found in a recent survey that the employees who are most likely to leave an organization are those with the most valuable skills. Studies show that highly competent employees choose workplaces that offer good career paths, state-of-the-art systems, training, and the chance to use their abilities to the fullest.

If federal agencies are to be effectively served in the future by information technology, the government must build a first-class work force. Responsibility for ensuring that this work force is in place falls directly on the government's top-level management, who must:

- Develop, as a high priority, a strategy to hire and train senior-level, technically oriented managers, and develop career paths

that will provide technically trained executives who can successfully introduce state-of-the-art technology throughout an organization.

- Develop strategies for recruiting and keeping technically skilled, junior-level staff.
- Establish special salary scales for technical personnel.

Top managers should also consider innovative approaches to focus expert technical talent on the critical issues discussed in this report. These approaches could include using advisory panels of senior industry executives experienced at introducing complex technology into organizations.

Related GAO Products

Managing IRS: Actions Needed to Assure Quality Service in the Future (GAO GGD-89-1, Oct. 14, 1988).

Environmental Protection Agency: Protecting Human Health and the Environment Through Improved Management (GAO/RCED-88-101, Aug. 16, 1988).

Social Security Administration: Stable Leadership and Better Management Needed to Improve Effectiveness (GAO/HRD-87-39, Mar. 18, 1987).

Department of Transportation: Enhancing Policy and Program Effectiveness Through Improved Management (GAO RCED-87-3, Apr. 13, 1987).

Justice Department: Improved Management Processes Would Enhance Justice's Operations (GAO GGD-86-12, Mar. 14, 1986).

Strong Leadership Needed to Improve Management at the Department of Labor (GAO HRD-86-12, Oct. 21, 1985).

Computer Procurement: Decision Needed on Navy's Standard Automated Financial System (GAO IMTEC-88-47, Sept. 13, 1988).

Military Space Operations: Shuttle and Satellite Computer Systems Do Not Meet Performance Objectives (GAO/IMTEC-88-7, Aug. 5, 1988).

Information Systems: Agencies Overlook Security Controls During Development (GAO/IMTEC-88-11, May 31, 1988).

Financial Markets: Status of Computer Improvements at the New York Stock Exchange (GAO/IMTEC-88-35, Apr. 27, 1988).

Federal Aviation Administration's Advanced Automation System Investment (GAO/T-IMTEC-88-3, Apr. 12, 1988).

Strong Leadership Needed to Revitalize Public Service (GAO/T-GGD-88-21, Mar. 24, 1988).

Command and Control: Upgrades Allow Deferral of $500 Million Computer Acquisition (GAO/IMTEC-88-10, Feb. 23, 1988).

ADP Modernization: IRS' Redesign of Its Tax Administration System (GAO/IMTEC-88-5FS, Nov. 9, 1987).

Information Management: Status of GSA's FTS 2000 Procurement (GAO/IMTEC-87-42, Aug. 24, 1987).

Hospital ADP Systems: VA Needs to Better Manage Its Decentralized System Before Expansion (GAO/IMTEC-87-28, July 24, 1987).

Air Force Computers: Development Risks of Logistics Modernization Program Can Be Reduced (GAO/IMTEC-87-19, May 15, 1987).

Information Management: Leadership Needed in Managing Federal Telecommunications (GAO/IMTEC-87-9, May 6, 1987).

ADP Systems: SSA's Modernization Efforts Need Redirection (GAO/IMTEC-87-16, Apr. 10, 1987).

Transition Series

The Budget Deficit (GAO/OCG-89-1TR).

The Public Service (GAO/OCG-89-2TR).

Revenue Options (GAO/OCG-89-3TR).

Financial Services Industry Issues (GAO/OCG-89-4TR).

International Trade Issues (GAO/OCG-89-5TR).

Information Technology Issues (GAO/OCG-89-6TR).

Financial Management Issues (GAO/OCG-89-7TR).

Program Evaluation Issues (GAO/OCG-89-8TR).

Defense Issues (GAO/OCG-89-9TR).

Health and Human Services Issues (GAO/OCG-89-10TR).

Commerce Issues (GAO/OCG-89-11TR).

Agriculture Issues (GAO/OCG-89-12TR).

Justice Issues (GAO/OCG-89-13TR).

Veterans Affairs Issues (GAO/OCG-89-14TR).

NASA Issues (GAO/OCG-89-15TR).

Energy Issues (GAO/OCG-89-16TR).

Treasury Issues (GAO/OCG-89-17TR).

Education Issues (GAO/OCG-89-18TR).

Department of State Issues (GAO/OCG-89-19TR).

Environmental Protection Agency Issues (GAO/OCG-89-20TR).

Department of Labor Issues (GAO/OCG-89-21TR).

Housing and Urban Development Issues (GAO/OCG-89-22TR).

Foreign Economic Assistance Issues (GAO/OCG-89-23TR).

Interior Issues (GAO/OCG-89-24TR).

Transportation Issues (GAO/OCG-89-25TR).

Internal Revenue Service Issues (GAO/OCG-89-26TR).

Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202 275-6241

The first five copies of each report are free. Additional copies are $2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.